

Title: Blockchain and AI for Maritime IoT and Port Cybersecurity

- Journal: International Journal of Emerging Digital Systems
- Author(s): Kael Veyron
- Affiliation: School of Information Systems, Atlantic Research Institute
- Domain(s):
 - o Computer Science [cs]
 - o Economics and Finance [q-fin]
 - o Social and Information Networks [cs.SI]
- Date of publication: September 2025

Keywords: Maritime Cybersecurity, Blockchain, Artificial Intelligence, IoT, Port Security, Shipping Logistics, Threat Intelligence

Abstract

Maritime transport supports over 80 percent of global trade. Ports, shipping vessels, and logistics chains are increasingly connected through IoT devices for cargo tracking, navigation, and port operations. These digital systems improve efficiency but expose the maritime industry to cyberattacks. Recent incidents show ransomware and GPS spoofing disrupting shipping routes and port operations. Traditional centralized defenses cannot handle the scale and complexity of maritime IoT. This paper examines the role of blockchain and artificial intelligence (AI) in maritime cybersecurity. Blockchain ensures secure device identity, tamper-proof cargo records, and decentralized trust. AI provides anomaly detection, predictive monitoring, and adaptive response. Methodology combines case study analysis, blockchain simulation in port logistics, AI anomaly detection models, and integrated framework testing. Findings show potential for improved resilience, but barriers of cost, scale, and regulation remain. By 2035, blockchain-AI systems are expected to be standard in global maritime cybersecurity.

Methodology

The research used a four-step framework:

1. **Case Study Review:** Maritime cyber incidents between 2012 and 2023 were reviewed, including the 2017 NotPetya ransomware that disrupted Maersk and GPS spoofing against vessels in the Black Sea.
2. **Blockchain Testing:** Hyperledger Fabric was deployed in a simulated port logistics system. Cargo tracking, customs clearance, and device authentication were recorded on blockchain. Metrics measured throughput, latency, and fraud reduction.
3. **AI Models:** Machine learning models such as decision trees, deep neural networks, and reinforcement learning were trained on maritime IoT datasets. These included AIS (Automatic Identification System) navigation data, container sensor readings, and port traffic logs. Models were tested against simulated attacks, such as false data injection and unauthorized access attempts.
4. **Integration Simulation:** A virtual port with 5,000 IoT sensors, 1,000 cargo containers, and 100 autonomous cranes was modeled. Blockchain authenticated

device communications and logged cargo movements. AI monitored network traffic for anomalies. Performance was measured in detection accuracy, downtime reduction, and resilience to ransomware.

This methodology provided evidence of blockchain and AI potential in port and shipping cybersecurity.

Current Standing

Maritime systems face growing cyber threats. Ransomware has shut down port terminals, costing millions in delays. GPS spoofing has misled vessels, threatening collisions and cargo loss. Container tracking IoT devices have been compromised to alter location data, enabling cargo theft.

Blockchain improves integrity in maritime IoT. Immutable ledgers record cargo movements from origin to destination. Smart contracts automate customs checks and payments. In pilots, blockchain reduced cargo fraud by 60 percent. Some ports, such as Rotterdam and Singapore, already experiment with blockchain-backed logistics. Still, scalability is a barrier. Large ports process millions of containers annually, generating vast amounts of IoT events. Current blockchain frameworks struggle to keep pace.

AI strengthens anomaly detection and predictive defense. Models trained on AIS datasets identify unusual vessel movements that signal spoofing. Neural networks detect abnormal patterns in crane or port equipment activity, flagging potential malware. In tests, AI detected abnormal cargo sensor readings with recall above 90 percent. Yet AI suffers from false positives and explainability issues. Maritime operators hesitate to act on AI alerts without human validation.

Adoption is uneven. Wealthy ports invest in blockchain-AI pilots, while smaller ports lack funding. Shipping companies often operate on thin margins and resist large cybersecurity investments. Regulations remain fragmented, with inconsistent enforcement across regions.

Future Outlook

The future of maritime cybersecurity lies in blockchain and AI integration.

1. **Blockchain for Cargo and Device Identity:** By 2030, all containers will carry blockchain-enabled IoT tags that record temperature, location, and handling events. Port devices, including cranes and gateways, will use blockchain for identity

authentication. This will prevent counterfeit cargo and unauthorized equipment access.

2. **AI Threat Intelligence:** AI will expand from anomaly detection to predictive intelligence. Models will forecast risks of ransomware or cargo tampering before they occur. Reinforcement learning will optimize vessel routing based on predictive risk. By 2032, AI dashboards will be standard in port cybersecurity centers.
3. **Consortium Blockchains for Trade:** Global shipping alliances and customs agencies will form blockchain consortiums to share verified cargo data. Immutable ledgers will prevent falsified bills of lading and fraud. Insurance providers may require blockchain audit trails for coverage.
4. **Edge Computing at Ports:** IoT devices in cranes, trucks, and sensors will embed blockchain and AI chips. Authentication and anomaly detection will happen locally, reducing latency and ensuring continuous security even if central systems fail.
5. **Global Standards:** By 2035, the International Maritime Organization (IMO) will enforce blockchain-AI cybersecurity standards across all member nations. Compliance will be required for vessels and ports, ensuring consistency in security measures.
6. **Defense Collaboration:** Governments will integrate maritime blockchain-AI systems into national defense. Ports will serve as critical infrastructure nodes, with shared threat intelligence between navies and port authorities.

The outcome will be resilient maritime systems where cargo is secure, vessel navigation is protected, and ports can withstand ransomware and cyber sabotage.

Closing Remarks

Maritime trade is the lifeline of the global economy, but it is increasingly at risk from cyberattacks. Blockchain provides immutable trust in cargo records and device identity. AI adds anomaly detection and predictive defense. Together, they form a framework for maritime cybersecurity. Today's pilots highlight promise but also reveal barriers of scale, cost, and fragmented regulation. By 2035, blockchain-AI integration will be mandatory across ports and shipping networks, ensuring safe and resilient global trade.

References:

- Mirza, J. B., Hasan, M. M., Paul, R., Hasan, M. R., & Asha, A. I. (2025). AI-Driven Business Intelligence in Retail: Transforming Customer Data into Strategic Decision-Making Tools. *AIJMR-Advanced International Journal of Multidisciplinary Research*, 3(1).
- Hasan, M. R., Hasan, M. M., Mirza, J. B., Hassan, A., Paul, R., Khan, M. N., & Nikita, N. A. (2025). The Role of AI in Digital Marketing Analytics: Enhancing Customer Segmentation and Personalization in IT Service-Based Businesses. *AIJMR-Advanced International Journal of Multidisciplinary Research*, 3(1).
- Arafat, M. S., Mirza, J. B., Jony, M. A. M., Islam, R., Rafi, S. S., Jalil, M. S., & Hossen, F. (2024). Blockchain and IoT Integration for Secure Supply Chain Operations: Unlocking Real-Time Transparency and Business Continuity. *AIJMR-Advanced International Journal of Multidisciplinary Research*, 2(6).
- Hassan, A., Hasan, M. M., Mirza, J. B., Paul, R., & Hasan, M. R. (2025). Optimizing IT Service Delivery with AI-Powered Digital Marketing Analytics: Understanding Client Needs for Enhanced Support Solutions. *AIJMR-Advanced International Journal of Multidisciplinary Research*, 3(1).